D0-prior

VERIFICATION OF TRANSLATION

I, Noriko Shimizu, translator of 2-2-35, Hiramatsu, Nara-City, Nara, Japan, hereby declare that I am conversant with the English and Japanese languages and am a competent translator thereof. I further declare that to the best of my knowledge and belief the following is a true and correct translation made by me of Japanese Patent Application No. 2000-381870 filed on December 15, 2000.

Date: November 16, 2005

Noriko Shimizu

NORIKO SHIMIZU

[CODE NO.] 100097445

[PATENT ATTORNEY]

[NAME] Fumio Iwahashi

[APPOINTED PATENT AGENT]

[CODE NO.] 100103355

[PATENT ATTORNEY]

[NAME] Tomoyasu Sakaguchi

[APPOINTED PATENT AGENT]

[CODE NO.] 100109667

[PATENT ATTORNEY]

[NAME] Hiroki Naito

[CHARGES]

[RECEIPT NO.] 011305

[AMOUNT] ¥21,000

[LIST OF ENCLOSURES]

[DOCUMENT]	Specification	1
[DOCUMENT]	Drawing	1
[DOCUMENT]	Abstract	1

[POWER OF ATTORNEY NO.] 9809938

storage means for storing the separated storage ECM and scrambled content;

ECM interpretation means for extracting a scrambling key list from the storage ECM;

scrambling key list interpretation means for extracting a scrambling key from the scrambling key list;

descrambling means for descrambling the scrambled content using the extracted scrambling key; and

reproduction means for reproducing the descrambled content.

[CLAIM 2]

The conditional access system of Claim 1,

the broadcast apparatus further comprising:

TS packetizing means for converting content into TS packets; and

TS packet counting means for acquiring one TS packet at a time, and counting an ordinal position of the acquired TS packet from a beginning of TS packets,

wherein the scrambling key list interpretation means extracts a scrambling key from the scrambling key list based on the counted ordinal position of the TS packet,

the reception apparatus further comprising

TS packet extraction means for acquiring one TS packet at a time from the scrambled content stored on the storage means, and counting an ordinal position of the acquired TS packet from a beginning of TS packets as a TS packet index,

wherein the scrambling key list interpretation means extracts a scrambling key from the scrambling key list based on the TS packet

a time from the scrambled content stored on the storage means and acquiring specific unscrambled information of the TS packet,

wherein the scrambling key list interpretation means extracts the scrambling key from the scrambling key list based on the specific unscrambled information.

[CLAIM 7]

The conditional access system of Claim 6,

the broadcast apparatus further comprising

scrambling key identifier calculation means for performing an operation on the specific unscrambled information,

wherein the scrambling key list interpretation means extracts a scrambling key from the scrambling key list based on the specific unscrambled information on which the operation has been performed, and

the reception apparatus further comprising

scrambling key identifier calculation means for performing an operation on the specific unscrambled information,

wherein the scrambling key list interpretation means extracts a scrambling key from the scrambling key list based on the specific unscrambled information on which the operation has been performed.

[CLAIM 8]

A reception apparatus comprising:

separation means for separating a storage ECM and scrambled content from a received pay broadcast program;

storage means for storing the separated storage ECM and scrambled content;

ECM interpretation means for extracting a scrambling key list

a scrambling key acquisition step for acquiring a scrambling key;

a scrambling key list generation step for generating a scrambling key list based on the scrambling key;

an ECM generation step for generating a storage ECM including the scrambling key list;

an ECM transmitting step for transmitting the storage ECM periodically;

a scrambling key list interpretation step for extracting a scrambling key from the scrambling key list;

a scrambling process step for scrambling content using the extracted scrambling key; and

a multiplexing step for multiplexing the storage ECM transmitted from the ECM transmitting means with the scrambled content to distribute a pay broadcast program,

the reception apparatus comprising:

a separation step for separating a storage ECM and scrambled content from a received pay broadcast program;

a storage step for storing the separated storage ECM and scrambled content;

an ECM interpretation step for extracting a scrambling key list from the storage ECM;

a scrambling key list interpretation step for extracting a scrambling key from the scrambling key list;

a descrambling process step for descrambling the scrambled content using the extracted scrambling key; and

a reproduction step for reproducing the descrambled content.

reproduction function such as a fast-forward reproduction function may not satisfy users.

[0004]

The invention aims to realize a special reproduction function after storage of scrambled content, at a level so as to satisfy users.

[MEANS TO SOLVE THE PROBLEMS]

[0005]

To solve the problems, the present invention is a conditional access system including a broadcast apparatus for distributing a pay broadcast program and a reception apparatus for receiving and reproducing the pay broadcast program, the broadcast apparatus being characterized by comprising: scrambling key acquisition means for acquiring a scrambling key; scrambling key list generation means for generating a scrambling key list based on the scrambling key; ECM generation means for generating a storage ECM including the scrambling key list; ECM transmitting means for transmitting the storage ECM periodically; scrambling key list interpretation means for extracting the scrambling key from the scrambling key list; scrambling means for scrambling content using the extracted scrambling key; and multiplexing means for multiplexing the storage ECM transmitted from the ECM transmitting means with the scrambled content to distribute a pay broadcast program, and the reception apparatus being characterized by comprising: separation means for separating the storage ECM and the scrambled content from the pay broadcast program received from the multiplexing means; storage means for storing the separated storage ECM and scrambled content; ECM interpretation means for extracting a scrambling key list from the storage ECM; scrambling

list holding unit 111, a scrambling unit 112, and a scrambling key list interpretation unit 113.

[0009]

To clarify a difference from a conventional BS digital broadcasting system, a system for generating an ECM and transmitting it in the conventional BS digital broadcasting system, which is different from a system for transmitting a storage ECM and generating it, is also shown in FIG. 1 and FIG. 2. Portions where a scrambling key acquired in the scrambling key acquisition unit 108 is passed to the scrambling process unit 103 and the ECM generation unit 104 correspond to the conventional BS digital broadcasting system (shown by dotted lines in the figures).

[0010]

FIG. 3 shows a construction of the descrambling process unit 204 of the receiver 200 in detail. The descrambling process unit 204 includes a TS packet extraction unit 210, a descrambling unit 211, and a scrambling key list interpretation unit 212.

[0011]

The following describes detailed operations of the broadcast apparatus and the receiver for describing correspondence information between TS packets and scrambling keys (information to extract a scrambling key corresponding to a TS packet from a scrambling key list) in an ECM (Entitlement Control Message).

[0012]

(Broadcast Apparatus)

FIG. 4 is a flowchart showing an operation procedure when scrambling content such as an image, a sound, and data in the broadcast

(Step S505). The scrambling process unit 103 scrambles the content converted into the TS packets (Step S506). The multiplexing unit 106 multiplexes the scrambled content with the storage ECM (Step S507) to generate a pay broadcast program. The pay broadcast program is broadcasted as a TS. In this specification, a pay broadcast program is defined as being generated by multiplexing scrambled content with a storage ECM.

[0013]

In the example of FIG. 1, a scrambling key and content are generated in an apparatus other than the broadcast apparatus 100. Instead, one or both of the scrambling key and the content may be generated in the broadcast apparatus 100.

[0014]

FIG. 5 is a detailed flowchart showing a process of the scrambling process unit 103 (Step S506 in FIG. 4). The scrambling process unit 103 acquires a scrambling key list from the scrambling key list generation unit 102, and stores it to the scrambling key list holding unit 111 (Step S601). The TS packet counting unit 110 acquires the content converted into TS packets by the TS packetizing unit 101 in Step S504, one TS packet at a time (Step S602). When acquiring the one TS packet, the TS packet counting unit 110 counts an ordinal position of the TS packet from a beginning of TS packets by accumulating the number of TS packets, passes a TS packet cumulative number (information of an ordinal position of a TS packet from a beginning of TS packets) to the scrambling key list interpretation unit 113, and passes the TS packet to the scrambling unit 112 (Step S603). The TS packet cumulative number is reset to zero before the process shown

is 101 since the TSP101 is a 101st TS packet. In accordance with the scrambling key list in FIG. 1, a scrambling key corresponding to the TSP101 is not the Ks1 but a next Ks2.

[0017]

(Timing for Transmitting Scrambling Key List)

The following describes a timing for transmitting the scrambling key list. Since at least one scrambling key list may be stored for each piece of scrambled content, the scrambling key list may be transmitted in a time period longer than a transmission period for the conventional BS digital broadcasting systems (for example, approximately ten times longer) as shown in FIG. 19. In an environment where the scrambling key list is assured to be securely stored, one scrambling key list may be transmitted for the scrambled content only once.

[0018]

(Receiver)

FIG. 6 is a flowchart showing an operation procedure in distinguishing between the storage ECM and the conventional ECMs based on the table identifier or the extended table identifier to separate the storage ECM and the scrambled content in the TS separation unit 201, storing the storage ECM in the HDD 202, and then descrambling the scrambled content in the receiver 200. The operation procedure is described with reference to FIG. 1 and FIG. 3. The storage ECM and the scrambled content may be stored as one TS temporarily, and then separated.

[0019]

The storage ECM stored on the HDD 202 is transmitted to the

(Detailed Operation of Receiver in Reproducing Scrambled Content in Special reproduction Mode)

The following describes a detailed operation of the receiver in reproducing the scrambled content after storage in a special reproduction mode. Here, a fast-forward reproduction mode, which is a typical special reproduction mode, is described. As shown in FIG. 21, in accordance with MPEG-2 coding system, an image stream includes three kinds of pictures: an I picture (an intraframe-coded picture), a B picture (a bidirectional frame), and a P picture (a predictive picture). Since only the I picture can be decoded solely, the fast-forward reproduction mode can be realized by reproducing only the I picture. FIG. 12 is a pattern diagram showing the image stream shown in FIG. 21 converted into a TS. In FIG. 12, it is simply presumed that I pictures in FIG. 21 are converted into the TS packets, being shaded portions in FIG. 12. That is, it is presumed that a first, second, third, and forth pictures are converted into packets from a TSP2 to a TSP5, packets from a TSP101 to a TSP104, packets from a TSP201 to a TSP204, and packets from a TSP301 to a TSP304, respectively.

[0022]

The following describes an operation procedure of the receiver in descrambling the TS packets, being the diagonally shaded portions. The scrambling key list is shown in FIG. 11. Although a flow of the operation procedure is the same as that in FIG.6, the process of the descrambling process unit is partly altered. Therefore, FIG. 22 shows the process of the descrambling process unit. The operation procedure is described with reference to FIG.7. The TS packet extraction unit 210 extracts scrambled content for one TS packet (Step S1101), and

by reversing an extraction order of TS packets in a fast-forward reproduction function. Also, a random access function is realized by altering a starting position of the TS packet to be extracted.

Various special reproduction modes is realized by extracting a scrambling key corresponding to any one of TS packets, a target to be descrambled, from the scrambling key list.

[0025]

(SECOND EMBODIMENT)

In the example of the first embodiment, security is assured within the receiver. The description is done with the construction that the scrambling key list holding unit 203 and the scrambling key list interpretation unit 212 are within the receiver. However, as shown in a construction of FIG. 13, if the scrambling key list holding unit 203 and the scrambling key list interpretation unit 212 are set within the security module 300, security of the scrambling key list can be improved. FIG. 14 shows the descrambling process unit in detail.

[0026]

Although a flow of an operation procedure in FIG. 14 is the same as those in FIG.6 and FIG. 7 (the process of the descrambling process unit in FIG. 6 (Step S705) is altered to a process of the descrambling process unit and the security module in FIG. 14), Step S803 in FIG. 7 is altered to a process of the security module in FIG. 14. In Step S803, the scrambling key may be encoded when passing the scrambling key from the security module 300 to the descrambling unit. The encoded scrambling key may be deleted from a memory within the receiver immediately after the process in the receiver

[0027]

[0031]

The descrambling process unit 204 includes a TS packet extraction unit 220, a scrambling key identifier calculation unit 221, a descrambling unit 222, and a scrambling key list interpretation unit 223.

[0032]

(Broadcast Apparatus)

A flowchart showing an operation procedure in scrambling content including an image, a sound, and data in the broadcast apparatus 100 is the same as the flowchart in FIG. 4. However, since the process in the scrambling process unit 103 (Step S505) is different from that in FIG. 4, FIG. 17 shows a flowchart of the operation procedure. The operation procedure is described with reference to FIG. 1 and FIG. 15.

[0033]

The scrambling process unit 103 acquires a scrambling key from the scrambling key list generation unit 102, and stores it to the scrambling key list holding unit 122 (Step S901). The TS packet header interpretation unit 121 acquires content converted to TS packets by the TS packetizing unit 101 (Step S504) for one TS packet (Step S902). The TS packet header interpretation unit 121 reads a value of CC when acquiring the one TS packet, passes the read value to the scrambling key identifier calculation unit 120, and passes the TS packet to the scrambling unit 123 (Step S903).

The scrambling key identifier calculation unit 120 calculates a scrambling key identifier based on the value of the CC, and passes it to the scrambling key list interpretation unit 124 (Step S904).

key list again. For example, by changing the value of n to 4 without changing the scrambling key list as shown in FIG. 20, the value of the identifier can be any number between 0 and 3. As a result, scrambling keys to be used are Ks1, Ks2, Ks3, and Ks4. Note that the value of n may be a fixed value in advance as a calculation method, or the value may be described in the variable portion in the storage ECM shown in FIG. 8.

[0035]

Instead of using the value of CC, specific bits of PCR (Program Clock Reference) or OPCR (Original PCR), which are prescribed by the MPEG-2 coding system as an international standard as well as CC, may be used for calculating the scrambling key identifier. For example, by using the four-bit values in the PCR or OPCR, a scrambling key identifier may be calculated in a same manner as in the above process using the value of CC.

[0036]

Otherwise, instead of using an area whose usage has been already prescribed by the MPEG-2 coding system, the value of a scrambling key identifier may be described directly in an area where a user can utilize freely, such as a private data area in Adaptation Field.

[0037]

(Receiver)

A flowchart of an operation procedure that the TS separation unit 201 separates the storage ECM and the scrambled content, and stores them in the HDD202, and then the receiver 200 descrambles the scrambled content is the same as that in FIG. 6. However, since the process of the descrambling unit 204 (Step S705) is different from

[EFFECTS OF THE INVENTION]

In the present invention, by transmitting a scrambling key list, when reproducing scrambled content after storage, a scrambling key corresponding to any one of TS packets, being a reproduction target, can be extracted immediately from the scrambling key list.

[0041]

Since a transmission period of the scrambling key list may be longer, transmission capacity and a control process of transmission timing by the broadcast apparatus can be decreased easily.

[0042]

Usage of plural scrambling keys for one piece of content can assure a conventional security intensity.

[0043]

Storage of the scrambling key list within a security module can protect the scrambling key list from detection by a malicious user.

[0044]

As described above, a sufficient performance level of a special reproduction function after storage of scrambled content can be realized in a method where a security intensity is assured.

[BRIEF DESCRIPTION OF THE DRAWINGS]

FIG. 1 shows an overall construction of a system.

FIG. 2 shows a construction of a scrambling process unit in a first embodiment of the present invention.

FIG. 3 shows a construction of a descrambling unit in the first embodiment of the present invention.

FIG. 4 is a flowchart showing an operation procedure of a

scrambling process unit in the third embodiment of the present invention.

FIG. 18 is a flowchart showing an operation procedure of the descrambling process unit in the third embodiment of the present invention.

FIG. 19 shows timing for transmitting the scrambling key list.

FIG. 20 is a second figure showing a specific example of the scrambling key list.

FIG. 21 is a schematic view showing an image stream in MPEG-2 coding system.

FIG. 22 is a flowchart showing an operation procedure of the descrambling process unit in reproducing content in a fast-forward reproduction mode in the first embodiment of the present invention.

[NUMERICAL REFERENCES]

100. . . . broadcast apparatus

101. . . . TS papcketizing unit

102. . . . scrambling key list generation unit

103. . . . scrambling process unit

104. . . . ECM generation unit

105. . . . ECM transmitting unit

106. . . . multiplexing unit

107. . . . content acquisition unit

108. . . . scrambling key acquisition unit

110. . . . TS packet counting unit

111, 122, 203. . . . scrambling key list holding unit

112, 123. . . . scrambling unit

113, 124, 212, 223. . . . scrambling key list interpretation

[DOCUMENT] Abstract

[SUMMARY]

[AIM] To realize a special reproduction function after storage of scrambled content, at a level so as to satisfy users.

[MEANS TO ACHIEVE THE AIM]

An broadcast apparatus comprising: scrambling key list generation means for generating a scrambling key, ECM generation means for generating a storage ECM based on the scrambling key list, ECM transmitting means for transmitting the storage ECM, and scrambling means for scrambling content each TS packet, and a receiver comprising: ECM interpretation means for extracting a scrambling key list from the received storage ECM, scrambling key list interpretation means for extracting a scrambling key of a corresponding TS packet, and descrambling means for descrambling content each TS packet.

[SELECTED DRAWING] FIG. 1

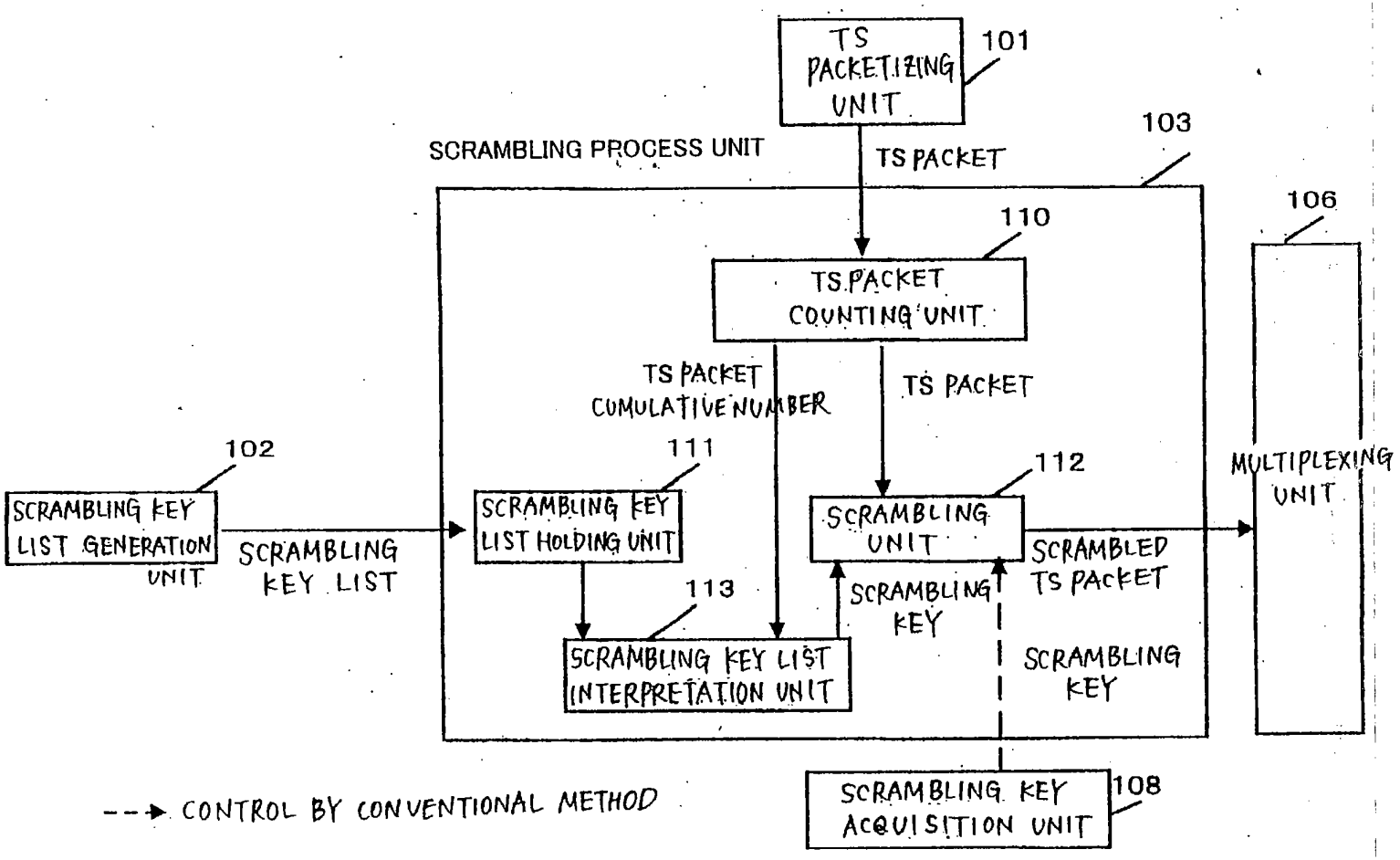

TS PACKETIZING UNIT
101
SCRAMBLING PROCESS UNIT
103
TS PACKET
106
110
TS PACKET COUNTING UNIT
TS PACKET CUMULATIVE NUMBER
TS PACKET
102
111
112
SCRAMBLING KEY LIST GENERATION UNIT
SCRAMBLING KEY LIST
SCRAMBLING KEY LIST HOLDING UNIT
SCRAMBLING UNIT
SCRAMBLED TS PACKET
MULTIPLEXING UNIT
113
SCRAMBLING KEY
SCRAMBLING KEY LIST INTERPRETATION UNIT
SCRAMBLING KEY
CONTROL BY CONVENTIONAL METHOD
SCRAMBLING KEY ACQUISITION UNIT
108

FIG. 2

FIG. 4

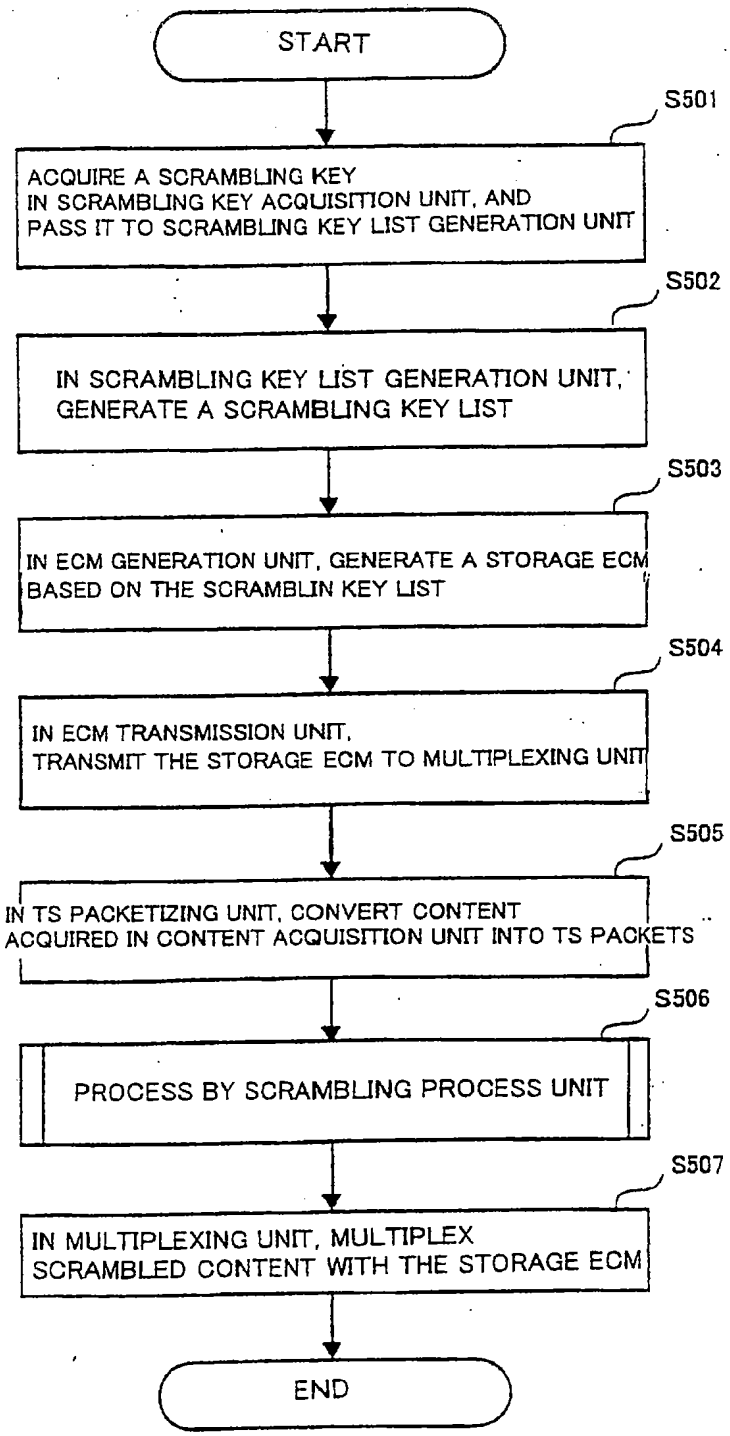

START
S501
ACQUIRE A SCRAMBLING KEY
IN SCRAMBLING KEY ACQUISITION UNIT, AND
PASS IT TO SCRAMBLING KEY LIST GENERATION UNIT
S502
IN SCRAMBLING KEY LIST GENERATION UNIT,
GENERATE A SCRAMBLING KEY LIST
S503
IN ECM GENERATION UNIT, GENERATE A STORAGE ECM
BASED ON THE SCRAMBLIN KEY LIST
S504
IN ECM TRANSMISSION UNIT,
TRANSMIT THE STORAGE ECM TO MULTIPLEXING UNIT
S505
IN TS PACKETIZING UNIT, CONVERT CONTENT
ACQUIRED IN CONTENT ACQUISITION UNIT INTO TS PACKETS
S506
PROCESS BY SCRAMBLING PROCESS UNIT
S507
IN MULTIPLEXING UNIT, MULTIPLEX
SCRAMBLED CONTENT WITH THE STORAGE ECM
END

FIG. 6

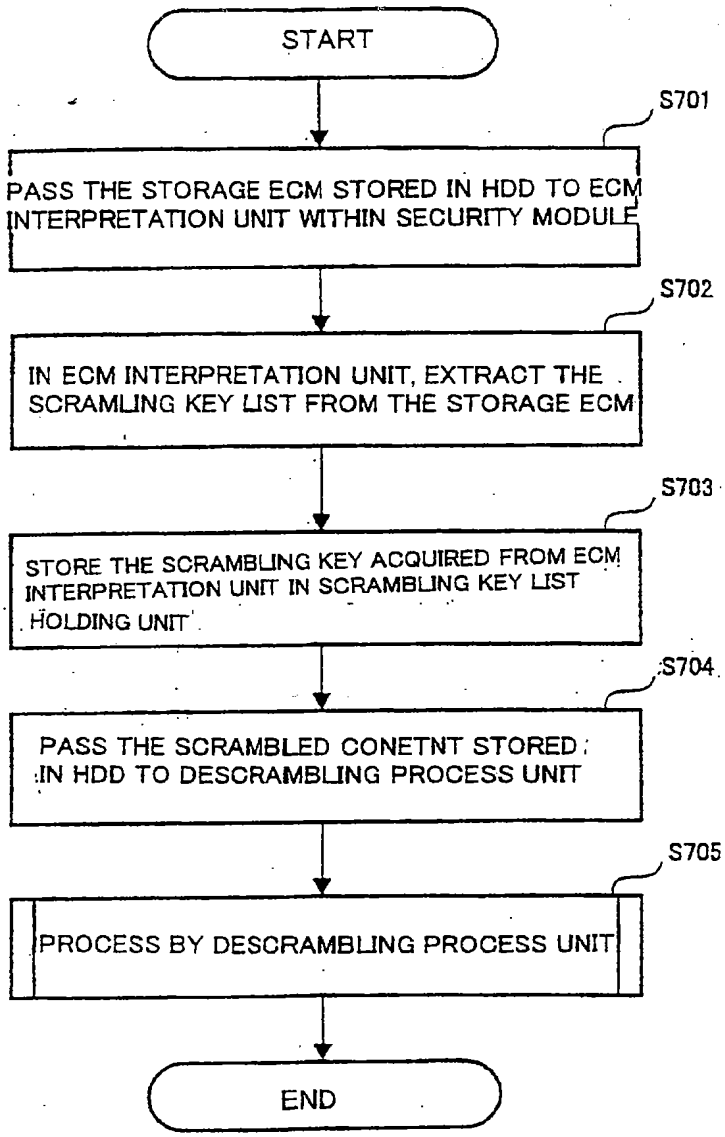

START
S701
PASS THE STORAGE ECM STORED IN HDD TO ECM INTERPRETATION UNIT WITHIN SECURITY MODULE
S702
IN ECM INTERPRETATION UNIT, EXTRACT THE SCRAMLING KEY LIST FROM THE STORAGE ECM
S703
STORE THE SCRAMBLING KEY ACQUIRED FROM ECM INTERPRETATION UNIT IN SCRAMBLING KEY LIST HOLDING UNIT
S704
PASS THE SCRAMBLED CONETNT STORED IN HDD TO DESCRAMBLING PROCESS UNIT
S705
PROCESS BY DESCRAMBLING PROCESS UNIT
END

FIG. 8

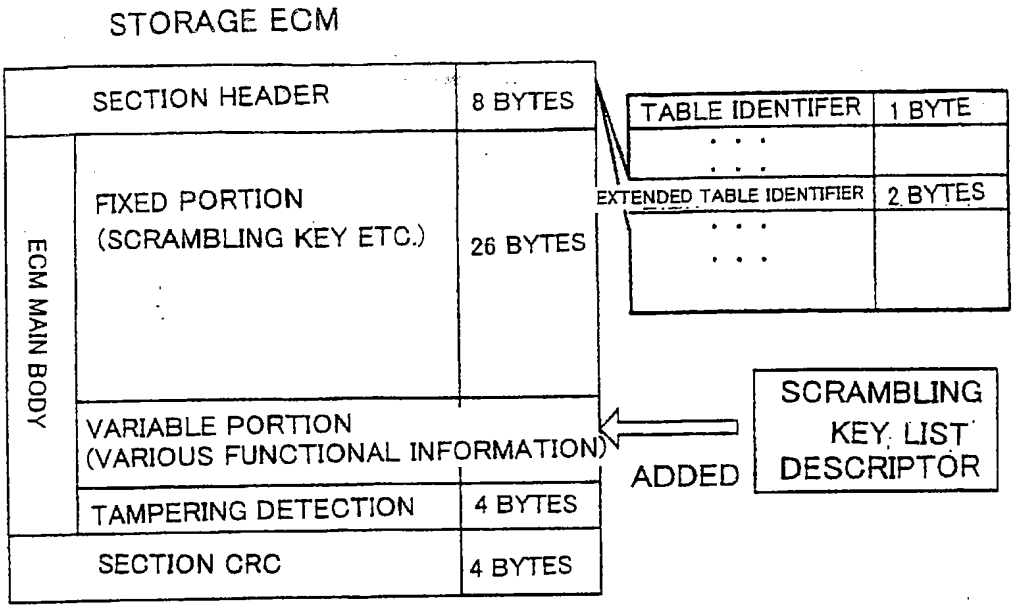


FIG. 9

DATA STRUCTURE OF SCRAMBLING KEY LIST DESCRIPTOR

CA_Ks_List_descriptor() {	
descriptor_tag	1 BYTE
descriptor_length	1 BYTE
for(i=0;i<N;i++) {	
Ks_id	1 BYTE
TS_packet_number	2 BYTES
Ks	8 BYTES
}	
}	

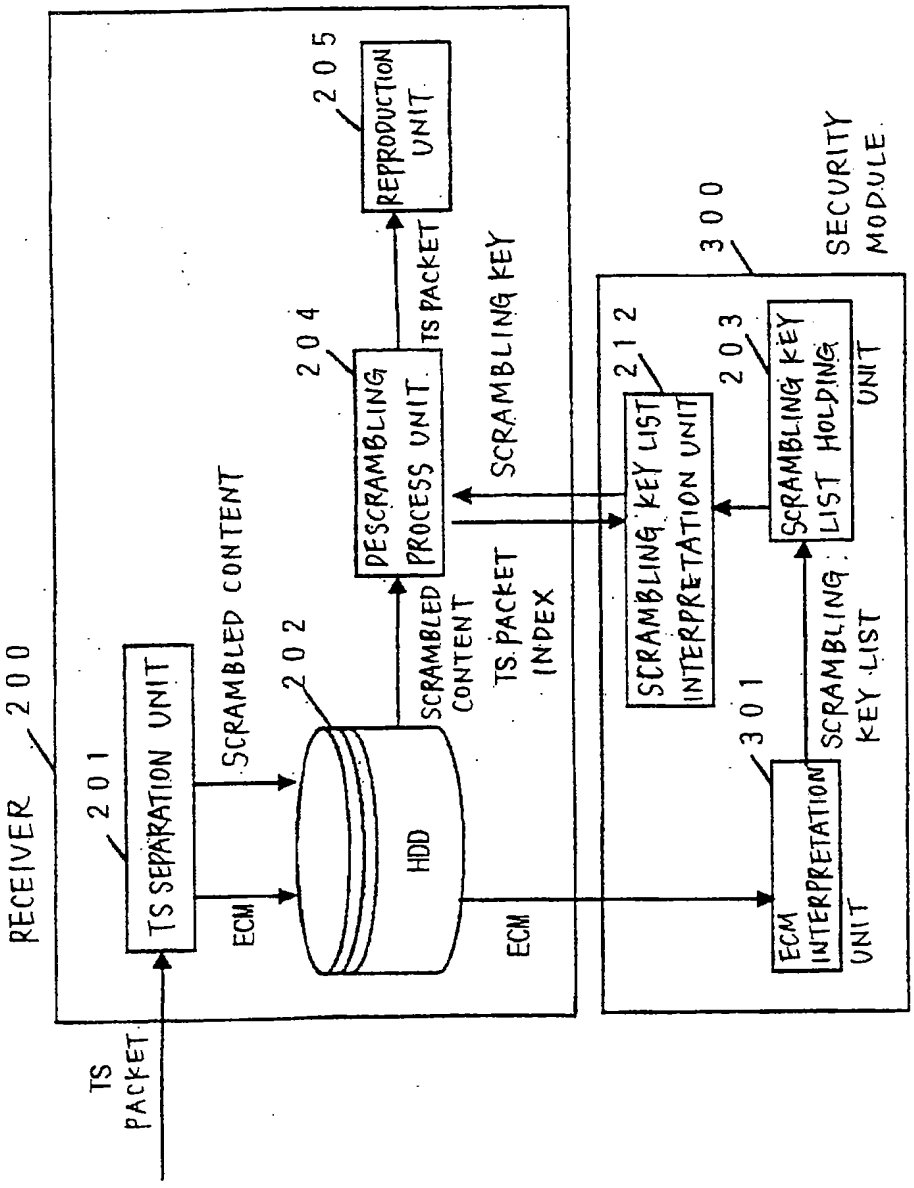
Ks_id : SCRAMBLING KEY IDENTIFIER (TO IDENTIFY SCRAMBLING KEYS)
TS_packet_number : THE NUMBER OF TS PACKETS SCRAMBLED WITH THE Ks
Ks : SCRAMBLING KEY

FIG. 11

SCRAMBLING KEY LIST

Ks_id	1
TS_packet_number	1 0 0
Ks	K s 1
Ks_id	2
TS_packet_number	1 0 0
Ks	K s 2
Ks_id	3
TS_packet_number	1 0 0
Ks	K s 3
Ks_id	4
TS_packet_number	1 0 0
Ks	K s 4

FIG. 13


RECEIVER
200
TS PACKET
TS SEPARATION UNIT
201
SCRAMBLED CONTENT
ECM
HDD
202
SCRAMBLED CONTENT
TS PACKET INDEX
ECM
DESCRAMBLING PROCESS UNIT
204
TS PACKET
REPRODUCTION UNIT
205
SCRAMBLING KEY
SCRAMBLING KEY LIST INTERPRETATION UNIT
212
SCRAMBLING KEY LIST HOLDING UNIT
203
ECM INTERPRETATION UNIT
301
SCRAMBLING KEY LIST
SECURITY MODULE
300

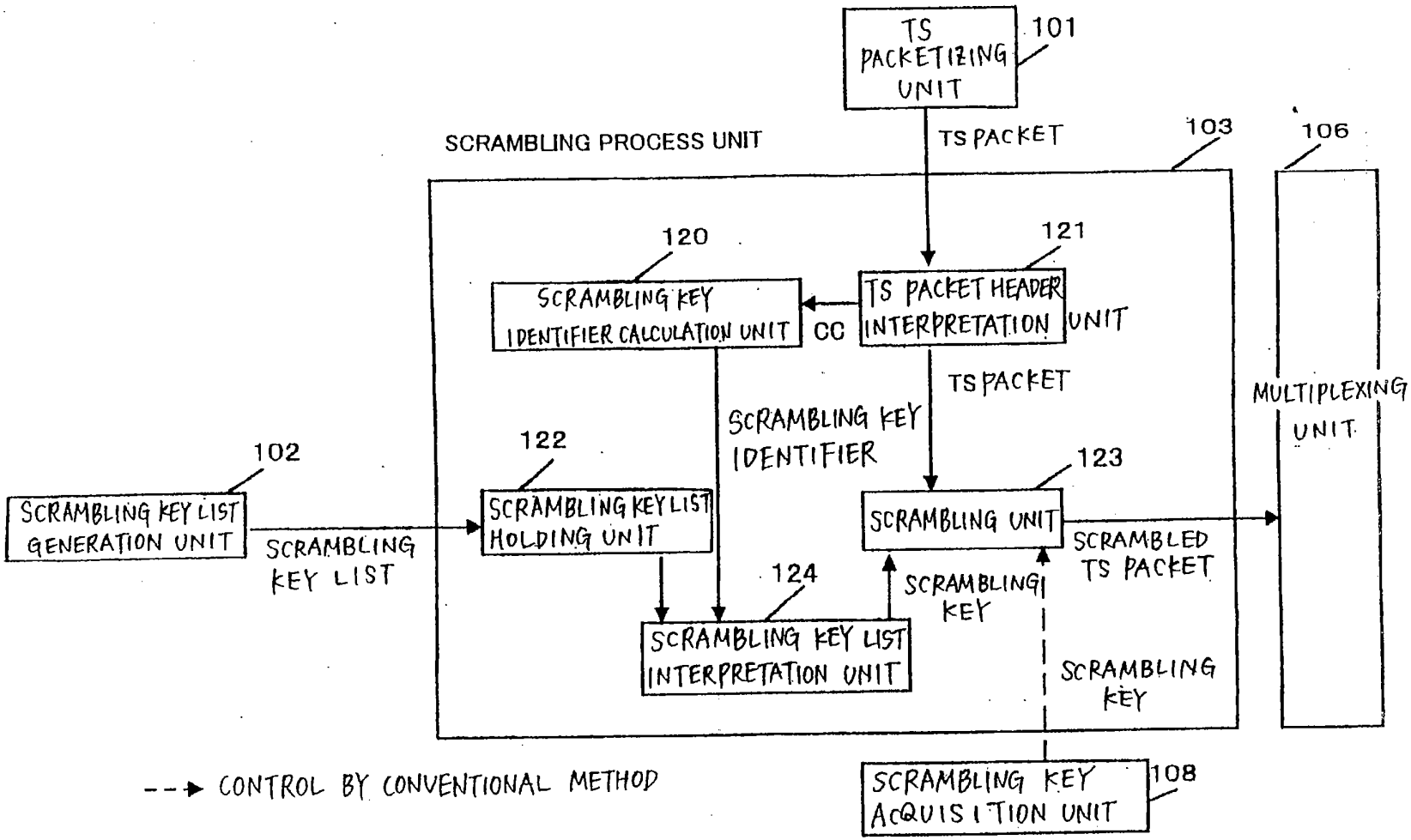
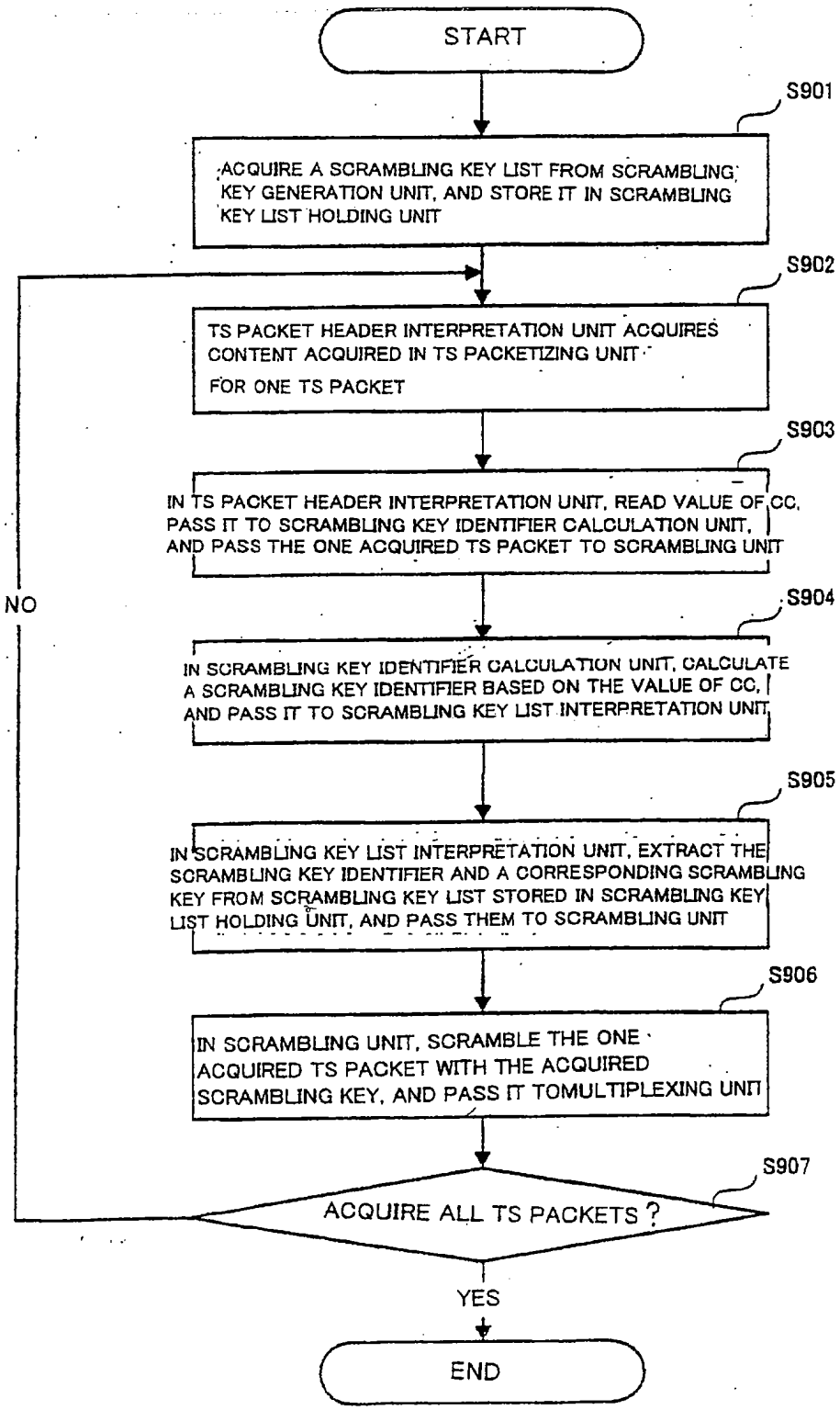
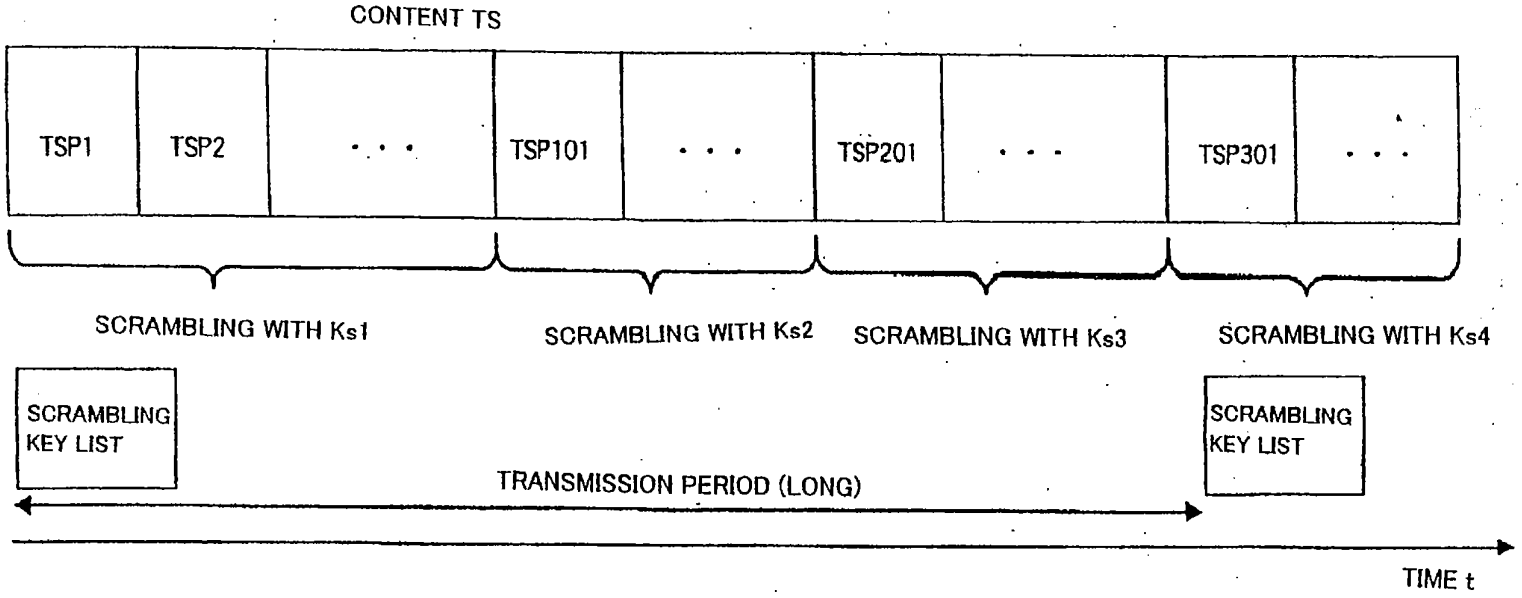

TS PACKETIZING UNIT
101
SCRAMBLING PROCESS UNIT
TS PACKET
103
106
120
121
SCRAMBLING KEY IDENTIFIER CALCULATION UNIT
CC
TS PACKET HEADER INTERPRETATION UNIT
TS PACKET
MULTIPLEXING UNIT
SCRAMBLING KEY IDENTIFIER
122
102
123
SCRAMBLING KEY LIST GENERATION UNIT
SCRAMBLING KEY LIST HOLDING UNIT
SCRAMBLING UNIT
SCRAMBLED TS PACKET
SCRAMBLING KEY LIST
124
SCRAMBLING KEY
SCRAMBLING KEY LIST INTERPRETATION UNIT
SCRAMBLING KEY
--→ CONTROL BY CONVENTIONAL METHOD
SCRAMBLING KEY ACQUISITION UNIT
108

FIG. 15

FIG. 17


START
S901
ACQUIRE A SCRAMBLING KEY LIST FROM SCRAMBLING KEY GENERATION UNIT, AND STORE IT IN SCRAMBLING KEY LIST HOLDING UNIT
S902
TS PACKET HEADER INTERPRETATION UNIT ACQUIRES CONTENT ACQUIRED IN TS PACKETIZING UNIT FOR ONE TS PACKET
S903
IN TS PACKET HEADER INTERPRETATION UNIT, READ VALUE OF CC, PASS IT TO SCRAMBLING KEY IDENTIFIER CALCULATION UNIT, AND PASS THE ONE ACQUIRED TS PACKET TO SCRAMBLING UNIT
S904
IN SCRAMBLING KEY IDENTIFIER CALCULATION UNIT, CALCULATE A SCRAMBLING KEY IDENTIFIER BASED ON THE VALUE OF CC, AND PASS IT TO SCRAMBLING KEY LIST INTERPRETATION UNIT
S905
IN SCRAMBLING KEY LIST INTERPRETATION UNIT, EXTRACT THE SCRAMBLING KEY IDENTIFIER AND A CORRESPONDING SCRAMBLING KEY FROM SCRAMBLING KEY LIST STORED IN SCRAMBLING KEY LIST HOLDING UNIT, AND PASS THEM TO SCRAMBLING UNIT
S906
IN SCRAMBLING UNIT, SCRAMBLE THE ONE ACQUIRED TS PACKET WITH THE ACQUIRED SCRAMBLING KEY, AND PASS IT TOMULTIPLEXING UNIT
S907
ACQUIRE ALL TS PACKETS ?
NO
YES
END

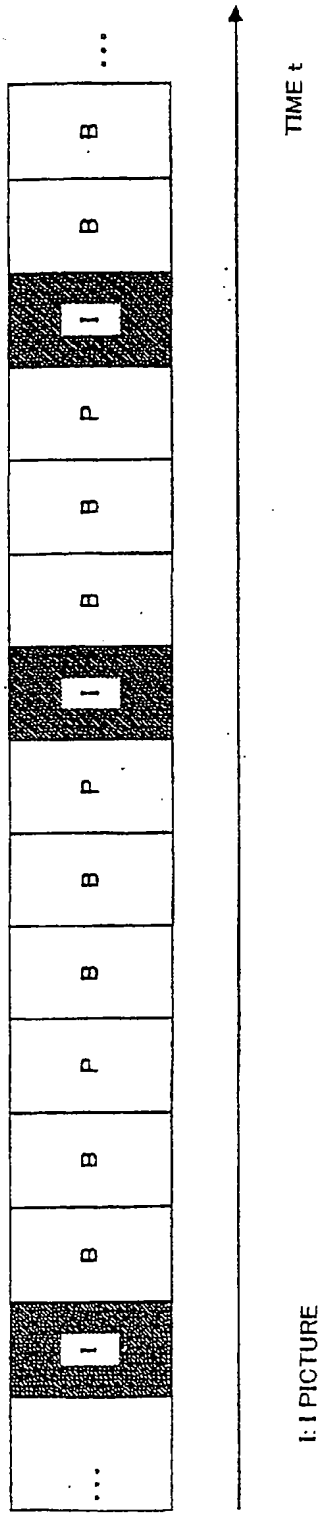


TS: TS PACKET

Ks: SCRAMBLING KEY

FIG. 19

FIG. 21


...
I
B
B
P
B
B
P
B
B
I
B
B
P
B
B
I
B
B
...
TIME t
I: I PICTURE
B: B PICTURE
P: P PICTURE